...mentary is excerpted from an article in the March Ma'arachot, a Hebrew-language scholarly journal published by the IDF.

...national will and capacity to wield decisive force. Only when they understand Israel is willing to "go all the way" are they deterred from rocket launches, terror attacks and other acts of so-called resistance.

...battling in the court of public opinion and are willing to sacrifice their citizens to promote their objectives. In contrast, Israel must wage three simultaneous battles: Maximize military achievements beyond our border; defend our population and its quality of life; and work to protect the uninvolved civilians on the other side who are cynically endangered by their own leaders.

...fulfillment of the new Middle East, decades of deterrence may crumble with the emergence of new regimes. We don't know what kind of regime will sprout from the nearly two-year civil war raging in Syria.

And with Egypt now controlled by the Muslim Brotherhood, we certainly must take into account the renewal of a long-dormant Western front. In that event, Israel will have no technological or qualitative edge.

...detecting and striking its leaders at any time in any place, even if he intentionally seeks cover in dense civilian areas.

In asymmetrical war, airpower is further challenged by the limited number of appropriate targets. Airpower delivers its most significant achievements in the opening days — if not hours or minutes — of the campaign. This was the case during the 2006 Lebanon War and also in ...

...gression. Conversely, disappointments and failings ascribed to the 2006 Lebanon War have delivered more than six years of quiet along our northern border.

What is clear is that three months after Pillar of Defense's unprecedented display of air power, quiet is prevailing across our southern border and life has returned to normal for the more than 1 million Israelis within rocket range. □

Time To Confront China's Cyber Espionage

As the administration of U.S. President Barack Obama prepared to unveil its plan to combat theft of American intellectual property, a computer network security company provided an instant litmus test for the new policy.

By **David Smith**, senior fellow and Cyber Center director at the Potomac Institute for Policy Studies, Arlington, Va.

Will Washington — administration and Congress — stand up to Chinese cyber espionage?

A sure indication will be whether we develop a comprehensive cybersecurity strategy or instead resort to tough rhetoric on Sunday morning talk shows and ineffective one-off measures.

On Feb. 19, Alexandria, Va.-based Mandiant published "APT1: Exposing One of China's Cyber Espionage Units." The company tracks dozens of advanced persistent threat (APT) groups, naming the most prolific of these organizations APT1.

APT1 has been stealing plans, processes, test results and business information from more than 141 companies since at least 2006. What is new in this report is that Mandiant researchers have convincingly matched the identity of APT1 to People's Liberation Army (PLA) Unit 61398.

Strategic cyber espionage poses three related challenges. First, general industrial espionage, likely driven by PLA investment in a broad spectrum of industries, debilitates our economy, even if an attack on, say, a large beverage producer is not an immediate threat to national security.

Second, plundering U.S. defense technology is a direct threat, tantamount to U.S. taxpayers underwriting the PLA's research-and-development budget such that we and our allies might someday face our own military technology in the field.

Third, in his Feb. 12 State of the Union address, Obama warned, "Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions and our air traffic control systems."

These three challenges are nothing less than a threat to America's world status.

However, the Mandiant report also delivers three bits of good news. Although the APT1 cyber espionage campaign is large, systematic and protracted, it is not particularly sophisticated. And having decided "to do our part to arm and prepare security professionals," Mandiant has helped forge a path toward the unprecedented government-business partnership necessary to secure America's cyber future.

Finally, the Mandiant report appears to be gaining bipartisan traction in Washington. If it galvanizes the country into action, we may have skirted the cyber "Pearl Harbor," which many observers speculate would be the only event likely to impel America to action.

However, devising effective actions will be hard. One obstacle is that until China is given a reason to do otherwise, it will simply stonewall. Heretofore, American grousing has come to naught. Mindful that the best defense is a good offense, Beijing has already categorically rejected Mandiant's findings.

"Making unfounded accusations based on preliminary results is both irresponsible and unprofessional," the Chinese Foreign Ministry stated. "China resolutely opposes hacking actions."

Rep. Eliot Engel, N.Y., ranking Democrat on the House Foreign Affairs Committee, has tried to raise the matter of Chinese hacking with Beijing officials. "They just let it roll off their back," he told ABC Television's "This Week." "They poohpoohed it."

To gain Beijing's serious attention, we will need considerably more than a few days of sharp rhetoric and a few visa denials. However, we must also not overplay our hand. With trade valued at $539 billion in 2011, China has risen to be our second-largest trading partner, which, at the end of 2012, held $1.2 trillion in U.S. Treasury bonds. Moreover, China's new leadership is months old, which may be both a challenge and an opportunity.

The goal will be to thread the needle with diplomacy that is tough and effective, and backed by the prospect of credible U.S. actions in case of further stonewalling. This is most likely to happen in the context of a comprehensive American cybersecurity strategy, which brings us to the second obstacle — Washington itself. It is time to pull together to take three steps.

First, we must calmly but decisively articulate a cybersecurity policy. We must explain to the American people and the world what is happening, the geopolitical context, the potential consequences and what we intend to do about it.

Second, we must build upon the Obama administration's "International Strategy for Cyberspace" with a comprehensive range of policy options and a clear message that we intend to exercise those options to safeguard our interests.

Finally, because threats will not evaporate, whether from China, Russia, Iran or others, government and business must work together to defend our critical infrastructure and our economy in general. Steps to maintain robust, resilient defenses must come from the private sector. Objectives, oversight and national coordination must come from government.

As we take the first steps to confront China in the coming weeks, these broader tasks may seem daunting, but they must be accomplished, and we can use the current situation as a start. □